

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED <div style="text-align: center;">Secret</div> b. LEVEL OF SAFEGUARDING REQUIRED																																																																																					
2. THIS SPECIFICATION IS FOR: (X and complete as applicable) a. PRIME CONTRACT NUMBER b. SUBCONTRACT NUMBER X c. SOLICITATION OR OTHER NUMBER N68836-16-T-0175			3. THIS SPECIFICATION IS: (X and complete as applicable) a. ORIGINAL (Complete date in all cases) DATE (YYYYMMDD) b. REVISED (Supersedes all previous specs) REVISION NO. DATE (YYYYMMDD) c. FINAL (Complete Item 5 in all cases) DATE (YYYYMMDD)																																																																																						
4. IS THIS A FOLLOW-ON CONTRACT? X YES <input type="checkbox"/> NO. If Yes, complete the following: Classified material received or generated under _____ (Preceding Contract Number) is transferred to this follow-on contract.			5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES X NO. If Yes, complete the following: In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____.																																																																																						
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code) a. NAME, ADDRESS, AND ZIP CODE b. CAGE CODE c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)																																																																																									
7. SUBCONTRACTOR a. NAME, ADDRESS, AND ZIP CODE b. CAGE CODE c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)																																																																																									
8. ACTUAL PERFORMANCE a. LOCATION COMNAVREG SOUTHEAST JACKSONVILLE, FL AND VARIOUS LOCATIONS THROUGHOUT THE SOUTHEAST REGION b. CAGE CODE c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) COMNAVREG SOUTHEAST BLDG 919 LANGLEY ST JACKSONVILLE, FL 32212																																																																																									
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT PROVIDE SUPPORT SERVICES TO FEDERAL ACTIVITIES UNDER GSA SCHEDULE IN SUPPORT OF COMNAVREG SOUTHEAST																																																																																									
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 40%;">10. CONTRACTOR WILL REQUIRE ACCESS TO:</th> <th style="width: 5%;">YES</th> <th style="width: 5%;">NO</th> <th style="width: 40%;">11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:</th> <th style="width: 5%;">YES</th> <th style="width: 5%;">NO</th> </tr> <tr> <td>a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION</td> <td></td> <td>X</td> <td>a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY</td> <td>X</td> <td></td> </tr> <tr> <td>b. RESTRICTED DATA</td> <td></td> <td>X</td> <td>b. RECEIVE CLASSIFIED DOCUMENTS ONLY</td> <td></td> <td>X</td> </tr> <tr> <td>c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION</td> <td></td> <td>X</td> <td>c. RECEIVE AND GENERATE CLASSIFIED MATERIAL</td> <td>X</td> <td></td> </tr> <tr> <td>d. FORMERLY RESTRICTED DATA</td> <td></td> <td></td> <td>d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE</td> <td></td> <td>X</td> </tr> <tr> <td>e. INTELLIGENCE INFORMATION</td> <td></td> <td></td> <td>e. PERFORM SERVICES ONLY</td> <td>X</td> <td></td> </tr> <tr> <td>(1) Sensitive Compartmented Information (SCI)</td> <td></td> <td>X</td> <td>f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES</td> <td></td> <td>X</td> </tr> <tr> <td>(2) Non-SCI</td> <td></td> <td>X</td> <td>g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER</td> <td></td> <td>X</td> </tr> <tr> <td>f. SPECIAL ACCESS INFORMATION</td> <td></td> <td>X</td> <td>h. REQUIRE A COMSEC ACCOUNT</td> <td></td> <td>X</td> </tr> <tr> <td>g. NATO INFORMATION</td> <td></td> <td>X</td> <td>i. HAVE TEMPEST REQUIREMENTS</td> <td></td> <td>X</td> </tr> <tr> <td>h. FOREIGN GOVERNMENT INFORMATION</td> <td></td> <td>X</td> <td>j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS</td> <td></td> <td>X</td> </tr> <tr> <td>i. LIMITED DISSEMINATION INFORMATION</td> <td>X</td> <td></td> <td>k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE</td> <td>X</td> <td></td> </tr> <tr> <td>j. FOR OFFICIAL USE ONLY INFORMATION</td> <td>X</td> <td></td> <td>l. OTHER (Specify)</td> <td></td> <td>X</td> </tr> <tr> <td>k. OTHER (Specify)</td> <td></td> <td>X</td> <td></td> <td></td> <td></td> </tr> </table>						10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO	a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		X	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	X		b. RESTRICTED DATA		X	b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X	c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X		d. FORMERLY RESTRICTED DATA			d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		X	e. INTELLIGENCE INFORMATION			e. PERFORM SERVICES ONLY	X		(1) Sensitive Compartmented Information (SCI)		X	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X	(2) Non-SCI		X	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		X	f. SPECIAL ACCESS INFORMATION		X	h. REQUIRE A COMSEC ACCOUNT		X	g. NATO INFORMATION		X	i. HAVE TEMPEST REQUIREMENTS		X	h. FOREIGN GOVERNMENT INFORMATION		X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		X	i. LIMITED DISSEMINATION INFORMATION	X		k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	X		j. FOR OFFICIAL USE ONLY INFORMATION	X		l. OTHER (Specify)		X	k. OTHER (Specify)		X			
10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO																																																																																				
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		X	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	X																																																																																					
b. RESTRICTED DATA		X	b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X																																																																																				
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X																																																																																					
d. FORMERLY RESTRICTED DATA			d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		X																																																																																				
e. INTELLIGENCE INFORMATION			e. PERFORM SERVICES ONLY	X																																																																																					
(1) Sensitive Compartmented Information (SCI)		X	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X																																																																																				
(2) Non-SCI		X	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		X																																																																																				
f. SPECIAL ACCESS INFORMATION		X	h. REQUIRE A COMSEC ACCOUNT		X																																																																																				
g. NATO INFORMATION		X	i. HAVE TEMPEST REQUIREMENTS		X																																																																																				
h. FOREIGN GOVERNMENT INFORMATION		X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		X																																																																																				
i. LIMITED DISSEMINATION INFORMATION	X		k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	X																																																																																					
j. FOR OFFICIAL USE ONLY INFORMATION	X		l. OTHER (Specify)		X																																																																																				
k. OTHER (Specify)		X																																																																																							

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (Specify)

Commander, Navy Region Southeast
Operations Director
Bldg 919, NAS Jacksonville, FL

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

1. Designated contractor employees to this contract shall be required to hold Secret Security Clearance for access to and handling of classified information. Designated contractors will require access to information up to and including SECRET and will require access to SIPRNET, which requires a security briefing.
2. Response Task Force (RTF) planners will require access to and will perform duties as designated in blocks 10 and 11 above.
3. Position requires employee to have access to classified material only at Government facility in performance of assigned duties.
4. Contractors will maintain all security information in JPAS, and submit appropriate classified visit requests as required.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. ☐ Yes ☒ No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. ☐ Yes ☒ No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL Jeanette Thomas	b. TITLE CNRSE Security Manager	c. TELEPHONE (Include Area Code) 904-542-1653
d. ADDRESS (Include Zip Code) COMNAVREG SOUTHEAST BLDG 919 LANGLEY ST JACKSONVILLE, FL 32212		17. REQUIRED DISTRIBUTION <input type="checkbox"/> a. CONTRACTOR <input type="checkbox"/> b. SUBCONTRACTOR <input type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR <input type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION <input type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER <input type="checkbox"/> f. OTHERS AS NECESSARY
e. SIGNATURE		

Block 8

Commander Navy Region Southeast
BLDG 919 Langley Street
NAS Jacksonville, FL 32212

Block 13 (Continued)

7. Ref 10e - DOD 5220.22-M, National Industrial Security Program Operating Manual, provides policy on control, access and dissemination of classified information. Contractor personnel shall have at a minimum an Interim Secret clearance based on a NACLIC investigation. Contractor (FSO) shall provide security training to cleared employees by initial briefings (including a Classified Information Non-disclosure Agreement (SF-312) , annual refresher briefings, and de-briefings. Prior approval of the government contracting agency (GCA) is required before a subcontract involving access to intelligence information can be issued.

8. Ref 10g - Office of the Under Secretary of Defense memorandum dated 5 December 2001, subject: Facilitating Necessary Access to NATO Classified Information, directs that all Department of Defense (DoD) military, civilian and contractor personnel briefed on their responsibilities for protecting US classified military information be briefed simultaneously on the requirements for protecting NATO classified information. The Contractor Facility Security Officer (FSO) shall provide a NATO awareness briefing to contractor personnel and shall maintain a written acknowledgment of the individual's receipt of the awareness briefing along with statement of understanding of responsibilities for safeguarding NATO classified information. There is not a defined requirement for NATO access to perform functions of this contract so Block 10g is checked "No". This briefing does not constitute "approval for access" and should not be entered in Joint Personnel Adjudication System (JPAS).

9. Ref Block 10j - For Official Use Only (FOUO) information received or generated under this contract shall be controlled and protected, marked, and safeguarded, as specified in DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM); SECNAVINST 5720.42F, Department of the Navy

Freedom of Information Act (FOIA) Program and SECNAV M-5510.36, DoN Information Security Program.

Block 13 (Continued)

10. Ref 10k - Contractor may have access to information that is protected under the Freedom of Information Act, Privacy Act and Personally Identifiable Information (PII) programs therefore identification is paramount and safeguarding shall be in accordance with SECNAVINST 5720.42F, Department of the Navy Freedom of Information Act (FOIA) Program and SECNAVINST 5211.5E, Department of the Navy Privacy Program.

11. Ref 11a - Contract access to classified information is restricted to specified Government Activity. All access to classified information shall be limited to that necessary to support work performance under this contract.

12. Ref 11e - Supply Technical Support Services performs tracking and storage. Classification markings on select media and local instruction will provide the classification guidance necessary for performance of this contract.

13. Ref 11j - OPNAVINST 3432.1A, Operations Security (OPSEC) provides basic guidance on OPSEC. The Contractor is not required to develop an OPSEC Plan. However, contractor personnel shall comply with all OPSEC plans and procedures in effect at all work locations. Contractor shall be made aware of the Commands Critical Information List (CIL) and Essential Elements of Friendly Information (EEFI) which shall be protected from public disclosure.

14. Ref 11l - Contractor positions on this work effort are designated "IT Systems Access" in accordance with NAVSUP Policy Letter 13-007, Contractor Unclassified Access to Federally Controlled Facilities, Sensitive Information, Information Technology Systems or Protected Health Information.

Block 13 (Continued)

15. Contractor personnel who currently have a favorably adjudicated NACLC investigation the contractor Facility Security Officer (FSO) will use the visitor certification program in the Joint Personnel Adjudication System (JPAS) to provide the individuals investigative information to the FLCY Security Manager. The Contractor will include the IT Position Category per SECNAV M-5510.30 for each person designated on a Visit Authorization Request. The VAR will be renewed annually or for the duration of the contract if less than one year.

16. In accordance with SECNAV M-5239.1, Department of the Navy Information Assurance (IA) Program; Initial IA Awareness training shall be provided to all military, civilian, and contractor personnel as a condition of access to DON information systems (NIS) in any system lifecycle phase. This training is available on-line and shall be taken upon work performance start date and annually thereafter for the duration of the contract.

17. Contractor personnel may require access to Navy Knowledge Online (NKO). The Contracting Officers Representative (COR) or Technical Point of Contact (TPOC) will provide sponsorship for this access.

18. Contractor personnel responsibility: Contractor personnel shall comply with all security policies and procedures for the protection of classified and sensitive information at all work locations. Contractor employees who handle U.S. Mail must do so IAW DODI 4525.08, DODI Official Mail Management and DODI 4525.7, Military Postal Service and Related Services. Warehouse Classified Material Handling will be IAW DOD 5220.22-M NISPOM and NAVSUPINST 5530.1 (series) Naval Supply Systems Command NAVSUP Security Manual.

Courier duties not assigned, courier card/letters will not be issued.

Block 13 (Continued)

The Government requiring activity will make Annual Counterintelligence Briefings available to all contractor personnel. Contractor personnel will attend the briefing at work performance start date and annually thereafter for the duration of the contract. Contractor personnel shall comply with all counterintelligence incident reporting requirements in

accordance with SECNAVINST 3850.2C, DoN Counterintelligence and as directed by Government requiring activity.

19. DOD 2000.12, DoD Antiterrorism (AT) Program requires annual antiterrorism training for all military, civilian employees and contractor personnel. The Government requiring conducts Level I training online at <https://Jkodirect.jten.mil>.

20. NAVSUP Policy Letter 13-007, Contractor Unclassified Access to Federally Controlled Facilities, Sensitive Information, Information Technology Systems or Protected Health Information; USD Memo (05DEC01) Facilitating Necessary Access to NATO Classified Information.